ENCIPHERING/DECODING METHOD

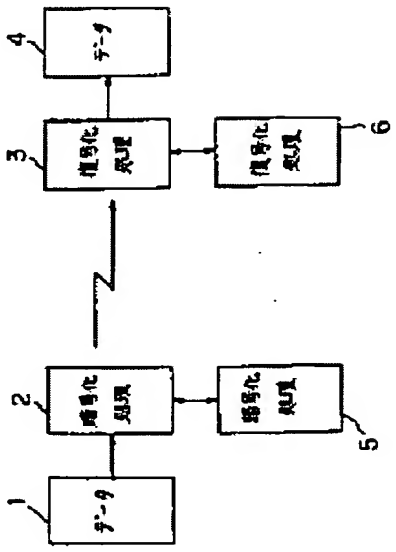
Patent number: JP3233792
Publication date: 1991-10-17
Inventor: TAJIMA HIROKI; KATO MAKOTO
Applicant: NIPPON DENKI OFFICE SYST
Classification:
- international: ***G06K17/00; G09C1/00; H04L9/00; H04L9/10; H04L9/12;*** **G06K17/00; G09C1/00; H04L9/00; H04L9/10; H04L9/12;** (IPC1-7): G06K17/00; G09C1/00; H04L9/00; H04L9/10; H04L9/12
- european:
Application number: JP19900030798 19900209
Priority number(s): JP19900030798 19900209

Report a data error here

Abstract of **JP3233792**

PURPOSE:To obtain the security of a high level in a data communication system by allowing an arithmetic processing of enciphering/decoding of data to depend on a software, and also, executing double enciphering/decoding by depending on a hardware or a firmware.

CONSTITUTION:Given data 1 is enciphered by executing an operation which depends on a software by an enciphering processing 2, it is sent to an enciphering processing 5 and encophered by executing an operation which depends on a hardware or a firmware, and the doubly enciphered data is returned to the enciphering processing 2, and transmitted to a receiving side through an interface circuit therefrom. In the receiving side, this data is received and sent to a decoding processing 6 through a decoding processing 3, and an operation which depends on a hardware or a firmware is executed therein, the data is decoded and returned to the decoding processing 3, and it is decoded by executing an operation which depends on a software, and restored to data 4 being equal to data 1 and outputted. In such a way, the security of a data communication system is improved.



Data supplied from the ***esp@cenet*** database - Worldwide

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−233792

⑤1Int.Cl.⁵	識別記号	庁内整理番号	④3公開　平成3年(1991)10月17日
G 06 K 17/00		6711−5B	
G 09 C 1/00	S	7230−5B	
H 04 L 9/00			
9/10			
9/12			
		6914−5K　H 04 L 9/00　Z	

審査請求　未請求　請求項の数 1　(全3頁)

⑤4発明の名称　暗号化・復号化方法

⑳特　願　平2−30798
㉒出　願　平2(1990)2月9日

⑦2発明者　田島　博貴　東京都港区芝5丁目7番15号　日本電気オフィスシステム株式会社内
⑦2発明者　加藤　誠　埼玉県浦和市田島8丁目4番19号　株式会社ジエム内
⑦1出願人　日本電気オフィスシステム株式会社　東京都港区芝4丁目13番2号
⑦4代理人　弁理士　内原　晋

明　細　書

1.発明の名称

暗号化・復号化方法

2.特許請求の範囲

1. データ通信における暗号化または復号化処理の暗号化・復号化方法において、

ソフトウェアに依存する演算による暗号化または復号化と、ハードウェアまたはファームウェアに依存する演算による暗号化または復号化とを加え、二重の暗号化または復号化を行うことを特徴とする暗号化・復号化方法。

3.発明の詳細な説明

〔産業上の利用分野〕

本発明はセキュリティを重視する各種データ通信に関し、特にプリペードカード、ICカード等に書き込むデータの暗号化または復号化の演算を行わせる為の暗号化・復号化方法に関する。

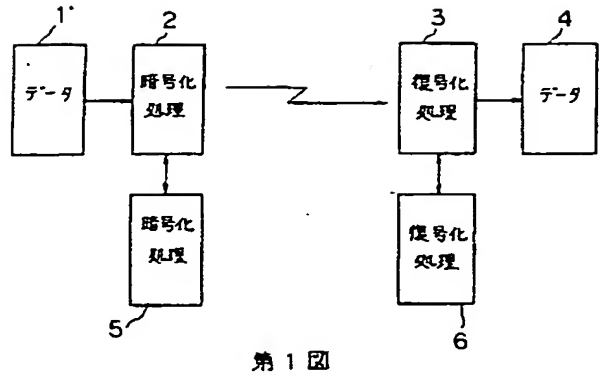
〔従来の技術〕

従来、この種の暗号化・復号化方法は、第3図に示すように、与えられたデータ1を暗号化処理2により、ソフトウェアだけに依存した演算を行って暗号化し、送信しており、これを受ける受信側においては、復号化処理3によりソフトウェアに依存する演算を行って復号化し、与えられたデータ1に等しいデータ4を出力していた。

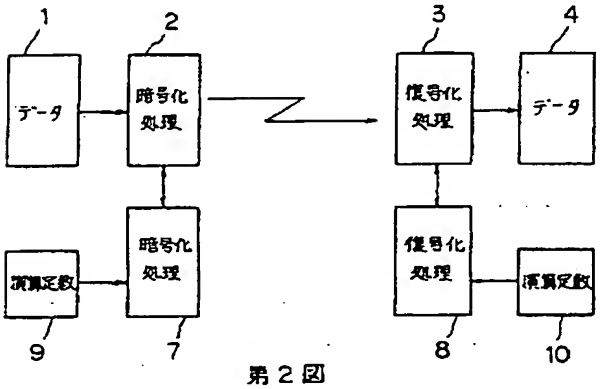
〔発明が解決しようとする課題〕

上述した従来の暗号化・復号化方法は、ソフトウェアだけに依存する演算が行われていた為に、プログラムの移植、改造や演算式の解読が容易に実行可能であるので、高いセキュリティが要求されるデータ通信システムを構成することは困難であるという欠点があった。

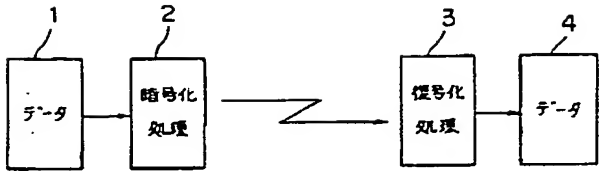
そこで本発明は、上記の欠点を解消してソフトウェアに依存する演算による暗号化または復号化だけでなく、これにハードウェアまたはファームウェアに依存する演算による暗号化または復号化を加えて二重に暗号化または復号化を行うことにより、プログラムの移植、改造や演算式解読が容易でなく、高いセキュリティを要求されてもこれに対応できる暗号化・復号化方法を提供すること


1
2
3
4
データ
暗号化処理
復号化処理
データ
暗号化処理
復号化処理
5
6

第1図


1
2
3
4
データ
暗号化処理
復号化処理
データ
演算定数
暗号化処理
復号化処理
演算定数
9
7
8
10

第2図


1
2
3
4
データ
暗号化処理
復号化処理
データ

第3図